UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,391	10/07/2003	Jong-Su Lim	44824	5463

7590 02/21/2008

Peter L. Kendall
Roylance, Abrams, Berdo & Goodman, L.L.P.
Suite 600
1300 19th Street, N.W.
Washington, DC 20036

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
02/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/679,391	LIM, JONG-SU	
	Examiner	Art Unit	
	SUMAN DEBNATH	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending in this application.

2. Claims 1-5 and 8-11 are presently amended in the amendment filed 28 March 2007.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/20/2007 has been entered.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5 and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release

4, 2001-08-28, hereinafter "DKS" and further in view of Hoffman (Patent No.: US 6,324,288 B1) and in view of Hoonjae Lee, "Parallel stream cipher for secure high-speed communications", 2001-07-09, hereinafter "Lee".

7. As to claim 1, DKS discloses an encryption method for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n, dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n, and generating a ciphertext bit stream of length 2n from the first, second, third and fourth sub-bit streams using 2-rounds of encryption (FIG. 1), the method comprising the steps of:

performing a first-round of encryption by encrypting the received first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting a second ciphertext bit stream encrypted again with a predetermined time delay right after the first ciphertext bit streams of length n are outputted (FIG. 2, FIG. 6, page 12, section 4.3);

generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream (FIG. 1, page 11, section 4.2, see also section 3.2);

generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream (FIG. 1, page 11, section 4.2, see also section 3.2); and

performing a second-round of encryption by encrypting the received first operated ciphertext bit stream and the second operated ciphertext bit stream comprising the predetermined time delay with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after encrypting the first operated ciphertext bit stream again predetermined second encryption codes (FIG. 2, FIG. 6, page 12, section 4.3, see also FIG. 1, page 11, sections 3.2, 4.1, 4.2).

DKS doesn't explicitly disclose performing encryption of first and second ciphertext bit stream at the same time. However, Lee discloses performing encryption of first and second ciphertext bit stream at the same time (page 262-263, section 2.3, Lee teaches this concept by identifying nonlinear functions to run these nonlinear functions combined in parallel).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of DKS by combining two nonlinear functions (i.e. two FO units) as taught by Lee in order to optimize speed or "faster processing (Lee, abstract)"

8. As to claim 2, DKS discloses wherein the predetermined first encryption codes comprises at least one of KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3 (page 12, section 4.3).

9. As to claim 3, DKS discloses the second predetermined encryption codes comprises at least one of KO.sub.2,1, KO.sub.2,2, KO.sub.2,3, KI.sub.2,1, KI.sub.2,2, and KI.sub.2,3 (page 12, section 4.3).

10. As to claim 4, DKS discloses the first-round encryption (FIG. 1) step comprises the steps of:

generating a first signal by performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1 to provide a first exclusive-OR operated bitstream, encrypting the first exclusive-OR-operated bit stream with the first encryption code KI.sub.1,1 to provide a first encrypted signal, and performing a logical exclusive-OR operation on the first encrypted signal and the second sub-bit stream, delayed by time required for the encryption (page 12, section 4.3, FIG. 2, 6);

generating the first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second sub-bit stream and the first encryption code KO.sub.1,2, to provide a second exclusive-OR operated bitstream encrypting the second exclusive-OR-operated bit stream with the first encryption code KI.sub.1,2, to provide a second encrypted signal, and performing a logical exclusive-OR-operation on the second encrypted signal and the first signal (page 12, section 4.3, FIG. 2, 6);

generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first signal and the first encryption code KO.sub.1,3 to provide a third exclusive-OR operated bitstream, encrypting the third exclusive-OR-operated bit stream with the first encryption code KI.sub.1,3, and performing a logical

exclusive-OR-operation on the encrypted signal with the first sub-bit stream delayed by time required for the encryption (page 12, section 4.3, FIG. 2, 6).

11. As to claim 5, DKA discloses the second-round encryption (FIG. 1) step comprises the steps of:

generating a second signal by performing a logical exclusive-OR-operation the first operated ciphertext bit stream and the second encryption code KO.sub.2,1 to provide a fourth exclusive-OR operated bitstream; encrypting the fourth exclusive-OR-operated bit stream with the second encryption code KI.sub.2,1 to provide a third encrypted signal, performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream (page 12, section 4.3, FIG. 2, 6);

generating the third operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit stream and the second encryption code KO.sub.2,2, encrypting the fifth exclusive-OR-operated bit stream with the second encryption code KI.sub.2,2, to provide a fourth encrypted signal; and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal; delayed by time required for the encryption (page 12, section 4.3, FIG. 2, 6); and

generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the second encryption code KO.sub.2,3, encrypting the sixth exclusive-OR-operated bit stream with the second encryption code KI.sub.2,3,

and performing a logical exclusive-OR-operation on the encrypted signal with the third ciphertext bit stream (page 12, section 4.3, FIG. 2, 6).

12. As to claim 7, DKA discloses the encryption method wherein a 16-bit input bit stream is divided into a 9-bit stream and a 7-bit stream, a 9-bit ciphertext bit stream is generated from the 9-bit stream using a first equation, and a 7-bit ciphertext bit stream is generated from the 7-bit stream using a second equation in each of the sub-encryptions (page 13-14, sections 4.5.1-4.5.2), wherein said first equation comprises

y 0 = (x0x2) ⊕ x3 ⊕ (x2x5) ⊕ (x5x6) ⊕ (x0x7) ⊕ (x1x7) ⊕ (x2x7) ⊕ (x4x8) ⊕ (x5x8) ⊕ (x7x8) ' ⊕1 ' ; y 1 = x1 ⊕ (x0x1) ⊕ (x2x3) ⊕ (x0x4) ⊕ (x1x4) ⊕ (x0x5) ⊕ (x3x5) ⊕ x6 ⊕ (x1x7) ⊕ (x2x7) ⊕ (x5x8) ' ⊕1 ' ; y2 = x1 ⊕ (x0x3) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x5x6) ⊕ (x4x7) ⊕ (x5x7) ⊕ (x6x7) ⊕ x8 ⊕ (x0x8) ' ⊕ 1 ' ; y3 = x0 ⊕ (x1x2) ⊕ (x0x3) ⊕ (x2x4) ⊕x5 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x4x7) ⊕ (x0x8) ⊕ (x1x8) ⊕ (x7x8) ; y4 = (x0x1) ⊕ (x1x3) ⊕x4 ⊕ (x0x5) ⊕ (x3x6) ⊕ (x0x7) ⊕ (x6x7) ⊕ (x1x8) ⊕ (x2x8) ⊕ (x3x8) ; y5 = x2 ⊕ (x1x4) ⊕ (x4x5) ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x7) ⊕ (x4x7) ⊕ (x6x7) ⊕ (x5x8) ⊕ (x6x8) ⊕ (x7x8) ' ⊕1 ' ; y6 = x0 ⊕ (x2x3) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x3x6) ⊕ (x4x6) ⊕ (x5x6) ⊕x7 ⊕ (x1x8) ⊕ (x3x8) ⊕ (x5x8) ⊕ (x7x8) ; y7 = (x0x1) ⊕ (x0x2) ⊕ (x1x2) ⊕ x3 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x4x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x2x7) ⊕ (x5x7) ⊕x8 ' ⊕1 ' ; y8 = (x0x1) ⊕x2 ⊕ (x1x2) ⊕ (x3x4) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x1x6) ⊕ (x4x6) ⊕ x7 ⊕ (x2x8) ⊕ (x3x8) (page 13-14, sections 4.5.1-4.5.2);

Second equation comprises y 0 = (x1x3) ⊕ x4 ⊕ (x0x1x4) ⊕ x5 ⊕ (x2x5) ⊕ (x3x4x5) ⊕ x6 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x2x4x6) ⊕ (x1x5x6) ⊕ (x4x5x6) ; y 1 = (x0x1) ⊕ (x0x4) ⊕ (x2x4) ⊕ x5 ⊕ (x1x2x5) ⊕ (x0x3x5) ⊕ x6 ⊕ (x0x2x6) ⊕ (x3x6) ⊕ (x4x5x6) ' ⊕ 1 ' ; y2 = x0 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x1x2x4) ⊕ (x0x3x4) ⊕ (x1x5) ⊕ (x0x2x5) ⊕ (x0x6) ⊕ (x0x1x6) ⊕ (x2x6) ⊕ (x4x6) ' ⊕ 1 ' ; y3 = x1 ⊕ (x0x1x2) ⊕ (x1x4) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x0x1x5) ⊕ (x2x3x5) ⊕ (x1x4x5) ⊕ (x2x6) ⊕ (x1x3x6) ; y4 = (x0x2) ⊕ x3 ⊕ (x1x3) ⊕ (x1x4) ⊕ (x0x1x4) ⊕ (x2x3x4) ⊕ (x0x5) ⊕ (x1x3x5) ⊕ (x0x4x5) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x0x3x6) ⊕ (x5x6) ' ⊕1 ' ; y5 = x2 ⊕ (x0x2) ⊕ (x0x3) ⊕ (x1x2x3) ⊕ (x0x2x4) ⊕ (x0x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x1x6) ⊕ (x1x2x6) ⊕ (x0x3x6) ⊕ (x3x4x6) ⊕ (x2x5x6) ' ⊕1 ' ; y6 = (x1x2) ⊕ (x0x1x3) ⊕ (x0x4) ⊕ (x1x5) ⊕ (x3x5) ⊕ x6 ⊕ (x0x1x6) ⊕ (x2x3x6) ⊕ (x1x4x6) ⊕ (x0x5x6) (page 13-14, sections 4.5.1-4.5.2) ;

13. As to claim 8, it is listed all the same elements of claims 1, 2 and 3 but in an encryption apparatus form rather than method form. DKS further discloses an encryption apparatus (FIG.1, which contains FL and FO units), first and second ciphering units (FIG. 1, FL unit) and operating unit (FIG.1, FIG. 2, FO unit). Therefore, the supporting rationales of the rejection to claim 1, 2 and 3 apply to claim 8.

14. As to claim 9, DKS discloses the encryption apparatus wherein the first ciphering unit (FIG. 1, item 210) comprises:

a first block having a first exclusive-OR operator for performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1, a first sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,1, and a second exclusive-OR operator for generating a first signal by performing a logical exclusive-OR operation on the encrypted signal with the second sub-bit stream being delayed to provide time for the encryption (page 12, section 4.3, FIG. 2, 6);

a second block having a third exclusive-OR operator for performing a logical exclusive-OR operation on the second sub-bit stream and the first encryption code KO.sub.1,2, a second sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,2, and a fourth exclusive-OR operator for generating the first operated ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the first signal; and a third block having a fifth exclusive-OR operator for performing a logical exclusive-OR operation on the first signal and the first encryption code KO.sub.1,3 (page 12, section 4.3, FIG. 2, 6),

a third sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,3, and a sixth exclusive-OR operator for generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the first sub-bit stream delayed by time required for the encryption (page 12, section 4.3, FIG. 2, 6).

15. As to claim 10, it is listed all the same elements of claim 5 but in an encryption apparatus form rather than method form. DKS further discloses an encryption apparatus (FIG.1, which contains FL and FO units) and blocks for processing bit streams (FIG. 2, 6, FI units). Therefore, the supporting rationales of the rejection to claim 5 apply to claim 10.

16. Claims 6 and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over DKS and further in view of Lee and Campbell, Jr. (Patent No.: 4,304,961), hereinafter "Campbell".

17. As to claim 6, DKS discloses each of the encryptions includes first and second sub-encryptions (FIG. 5).

Neither DKS nor Lee explicitly discloses outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal. However, Campbell discloses the outputs are stored and simultaneously retrieved according to an external clock signal (Campbell teaches the concept of storing and simultaneous retrieval according to clock signal, e.g. see, -FIG. 1A, items 18, 20, 22, FIG. 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of DKS and Lee as taught by Campbell in order to "provide and improved authenticator code generator for generating a unique authenticator code which is dependent on a key variable stored in the

authenticator code generator and the text of a received message" (Campbell, column 3, lines 45-49).

18. As to claim 11, it is listed all the same elements of claim 6 but in an encryption apparatus form rather than method form. DKS further discloses an encryption apparatus (FIG.1, which contains FL and FO units) and first and second sub-ciphering units (FIG. 5, S9 and S7 units). Therefore, the supporting rationales of the rejection to claim 6 apply to claim 11.

19. As to claim 12, it is listed all the same elements of claim 7 but in an encryption apparatus form rather than method form. DKS further discloses an encryption apparatus (FIG.1, which contains FL and FO units) and first and second sub-ciphering units (FIG. 5, S9 and S7 units). Therefore, the supporting rationales of the rejection to claim 7 apply to claim 12.

20. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part

of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/19/08